

ABSTRACT OF THE DISCLOSURE

It is an object of the present invention to provide a method and apparatus for solving key equation polynomials in the decoding of codewords. Based upon the Euclidean algorithm, it can be implemented with minimal hardware circuitry and provide a method and apparatus for solving key equation within a t-step iterative decoding procedure while the prior art architectures require at most $2t$ iterations. It is yet another object of the present invention to provide a method and apparatus for solving key equation polynomials without decreasing the overall decoding speed of the decoder. Briefly, in a presently invention, a method for computing error locator polynomial and error evaluator polynomial in the key equation solving step of the error correction code decoding process is presented whereby the polynomials are generated through at most t intermediate iterations that can be implemented with minimal amount of hardware circuitry. However, depending on the selected (N,K) code, the number of cycles required for the calculation of the polynomials would be within the time required for the calculation of upstream data. Additionally, a presently invention for computing the error locator polynomial and the error value polynomial employs an efficient scheduling of a small number of registers and finite-field multipliers (FFMs) without the need of finite-field inverters (FFIs) is illustrated. Using these new methods, a new area-efficient architecture that uses only $4t+2\rho+4$ registers and three FFMs and no FFIs is presented to implement the inversionless Euclidean algorithm. This method and architecture can be applied to a wide variety of RS and BCH codes with suitable code sizes.